the deleted user-token. Processing then continues to decision block 600 where the security steps of 600-606 are again initiated.

Steps 600-606 ensure that the speed and efficiency advantages of the access check system of the present invention do not result in security holes. The increased speed of the present invention is thereby implemented only when, from a security standpoint, it is safe to do so.

Summary

The access check system of the present invention includes a method and apparatus for efficiently accomplishing access checks for requested resources rather than performing a full, file-open, access check each time a user requests a resource. Although specific embodiments are disclosed herein, it is expected that persons skilled in the art can and will design alternative header generation systems that are within the scope of the following claims either literally or under the Doctrine of Equivalents.

We claim:

1. A computer-readable medium having computer-executable instructions for providing access to a computer network by performing steps comprising:

receiving a request from a user to access a resource on the computer network;

checking a first memory to determine if the user may access the resource;

providing the user with access to the resource if the first memory indicates that the user may access the resource;

checking a second memory to determine if the user may access the resource if the first memory does not indicate that the user may access the resource;

providing the user with access to the resource if the second memory indicates that the user may access the resource; and

storing information in the first memory indicating that the user may access the resource if, after checking the second memory, the second memory indicates that the user may access the resource.

2. The computer-readable medium of claim 1 wherein the first memory indicates that the user may access the resource by indicating that access to the resource has been previously provided to the user.

3. The computer-readable medium of claim 1 wherein the user is represented in the first memory by a token.

4. The computer-readable medium of claim 3 wherein the token also represents a plurality of other users.

5. The computer-readable medium of claim 3 wherein the token represents anonymous users.

6. The computer-readable medium of claim 3 further comprising:

authorizing fs to check the first memory.

7. The computer-readable medium of claim 1 wherein the resource is a file.

8. The computer-readable medium of claim 1 wherein the resource is a volume of files.

9. The computer-readable medium of claim 1 wherein the resource is a memory device.

Sub a2

10. The computer-readable medium of claim 1 wherein storing the information in the first memory comprises overwriting other information associated with the resource in the first memory.

11. The computer-readable medium of claim 10 wherein storing the information in the first memory comprises writing a token for the user in the first memory over another token for another user that had last previous access to the resource.

12. The computer-readable medium of claim 1 further comprising, if the resource is altered, removing indications from the first memory allowing access to the resource.

13. The computer-readable medium of claim 1 further comprising, if rights of the user are altered, removing indications from the first memory allowing access by the user.

14. The computer-readable medium of claim 1 wherein the request from the user indicates an operation to perform with respect to the resource, and further comprising:

checking the first memory to determine if the user may perform the operation with respect to the resource;

providing the user with access to the resource to perform the operation if the first memory indicates that the user may perform the operation with respect to the resource;

checking a second memory to determine if the user may perform the operation with respect to the resource if the first memory does not indicate that the user may perform the operation with respect to the resource;

providing the user with access to the resource if the second memory indicates that the user may perform the operation with respect to the resource; and

storing information in the first memory indicating that the user may perform the operation with respect to the resource if, after checking the second memory, the second memory indicates that the user may perform the operation with respect to the resource.

15. A method for providing access to a computer network, the method comprising:

receiving a request from a user to access a resource on the computer network;

checking a first memory to determine if the user may access the resource;

providing the user with access to the resource if the first memory indicates that the user may access the resource;

checking a second memory to determine if the user may access the resource if the first memory does not indicate that the user may access the resource;

providing the user with access to the resource if the second memory indicates that the user may access the resource; and

storing information in the first memory indicating that the user may access the resource if, after checking the second memory, the second memory indicates that the user may access the resource.

16. The method of claim 15 wherein the first memory indicates that the user may access the resource by indicating that access to the resource has been previously provided to the user.

17. The method of claim 15 wherein the user is represented in the first memory by a token.

18. The method of claim 17 wherein the token also represents a plurality of other users.

19. The method of claim 17 wherein the token represents anonymous users.

20. The method of claim 17 further comprising:

authorizing the user by checking a password provided by the user;

associating the token with the user after authorizing the user; and

using the token to check the first memory.

21. The method of claim 15 wherein the resource is a file.

22. The method of claim 15 wherein the resource is a volume of files.

23. The method of claim 15 wherein the resource is a memory device.

24. The method of claim 15 wherein storing the information in the first memory comprises overwriting other information associated with the resource in the first memory.

25. The method of claim 24 wherein storing the information in the first memory comprises writing a token for the user in the first memory over another token for another user that had last previous access to the resource.

26. The method of claim 15 further comprising, if the resource is altered, removing indications from the first memory allowing access to the resource.

27. The method of claim 15 further comprising, if rights of the user are altered, removing indications from the first memory allowing access by the user.

28. The method of claim 15 wherein the request from the user indicates an operation to perform with respect to the resource, and further comprising:

checking the first memory to determine if the user may perform the operation with respect to the resource;

providing the user with access to the resource to perform the operation if the first memory indicates that the user may perform the operation with respect to the resource;

checking a second memory to determine if the user may perform the operation with respect to the resource if the first memory does not indicate that the user may perform the operation with respect to the resource;

providing the user with access to the resource if the second memory indicates that the user may perform the operation with respect to the resource; and

storing information in the first memory indicating that the user may perform the operation with respect to the resource if, after checking the second memory, the second memory indicates that the user may perform the operation with respect to the resource.

add C5

add C10